Enabling Digital Transformation with Android

Providing a simple and secure way to meet any enterprise use case with Android and VMware Workspace ONE

AT A GLANCE

The combination of VMware Workspace ONE and Android provides a secure and consumer-simple experience to transform how work gets done.

KEY HIGHLIGHTS

- Streamlined configuration and deployment of Android work profile mode, fully managed device mode, and a work profile on a fully managed device.
- Enterprise security and end-user privacy for work apps and data, all configured from one console.
- Unified access to all apps including mobile Android apps with Google Play integration.

Why a Digital Workspace?

Today, mobile devices are being seen more and more in many aspects of businesses. With a wide range of form factors, mobile devices enable employees to be efficient and connected, regardless of location. And their uses are expanding to include even the most mission-critical operations of an organization. The rapid adoption of modern, mobile applications and the increasing demand for off-network connectivity creates challenges for IT. Devices must be secured and managed for organizations to enable access of apps and resources.

VMware Workspace ONE® is an intelligence-driven digital workspace platform that combines app delivery, access control, and unified endpoint management (UEM) for data security and end-user productivity. Admins are able to configure device policies, manage apps, and gain valuable insights into their device fleet from a unified console. The Workspace ONE application catalog gives end users one location to access all their applications—web, SaaS, native, or virtual—to be able to pick up where they left off from anywhere. To make it even simpler for the end user, admins can enable single sign-on (SSO) for fast and password-less access to their work critical apps.

Workspace ONE Enables Business Mobility on Android Devices

The Android operating system powers many types of devices from smartphones and tablets to ruggedized devices built for operations in harsher working environments. Android enterprise provides a modern management approach for enterprises and offers multiple deployment modes developed to suit a wide variety of use cases. It also maintains a consistent experience for end users, regardless of device manufacturer and form factor.

Workspace ONE UEM Support for Android Enterprise Deployment Modes

For BYOD deployments, a work profile can be delivered to devices to separate work apps and data on the device. Work apps are badged with an icon to visually signify to the end user which apps are managed by their organization. Employees have the ability to turn off their work profile to stop receiving work notifications at the end of the day or when they are on vacation.

Corporate devices can be enrolled out of the box and provisioned in fully managed device mode. Workspace ONE UEM integrates with each method of onboarding—QR code, NFC bump, EMM identifier, zero-touch enrollment, and Samsung Knox Mobile Enrollment—for flexibility based on device type and IT preference. Fully managed device mode enables IT to manage the entire device for additional control and security. These devices can be locked down to a single app or you can select multiple apps for dedicated device uses such as kiosks or rugged devices. The managed Google Play store on these devices is restricted to only corporate whitelisted apps.

For more flexibility on corporate-owned devices, enable the work profile for corporate-owned, personally enabled use cases. This deployment mode is enrolled out of the box like the fully managed device, but delivers badged corporate apps in the work profile and gives the end user the ability to install personal apps outside of the work profile.

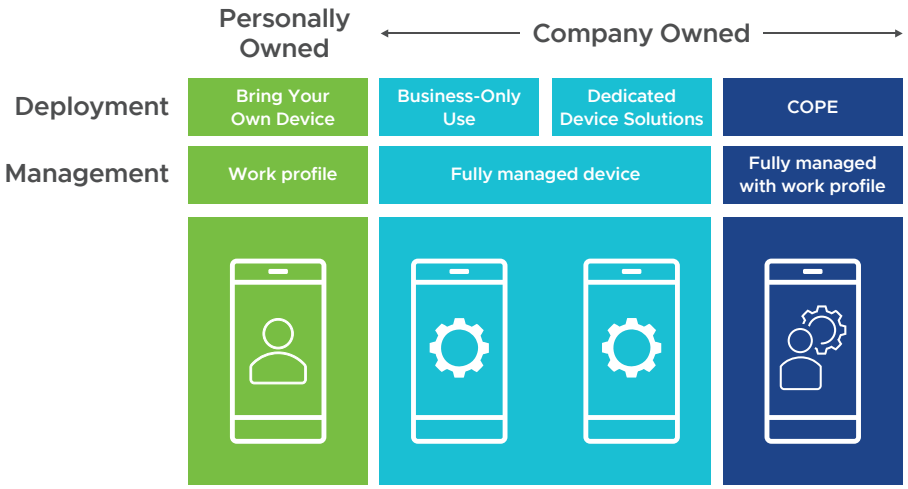

Figure 1: Flexible device management offers choice for IT.

Secure Management of Devices from One Console

From the unified Workspace ONE UEM console, administrators can send policies to devices and monitor their entire device fleet. The console is where admins integrate with Google to configure Android enterprise devices to deploy the work profile, fully managed device, and corporate-owned personally enabled device settings. With the automated compliance engine, rooted or non-compliant devices can be remediated with actions from sending notifications to enterprise wiping the device. When a work profile is deployed, administrators can set policies such as restricting the user from sharing data from a managed app to a personal app. Work security challenge enables work-managed applications to have a passcode for authentication and allows the admin to set the required passcode complexity without requiring a full device passcode.

Workspace ONE with Android also enables dedicated-device use cases such as rugged devices and kiosks. These devices can be locked down in fully managed device mode and provisioned with a single app or set of apps. Devices can even be configured for shared device mode, enabling users, such as shift workers, to check in and check out devices and get access to their assigned apps and resources. With VMware Workspace ONE Assist, IT and help desk staff can remotely view or control any Android device, directly from the Workspace ONE console, while maintaining employee privacy and trust.

LEARN MORE

Visit *www.vmware.com/products/workspace-one.html*, or call +1-877-4-VMWARE.

Single Location for All Apps

VMware Workspace ONE® Intelligent Hub is a self-service catalog for all applications including managed Android native apps. Workspace ONE integrates with Google Play both in the Workspace ONE UEM console and on the device for a truly seamless experience for both the admin and the end user. Google Play is directly embedded in the admin console, so the admin does not need to navigate to another location to approve work applications.

In addition, IT has the option to include a consumer-simple Workspace ONE suite of productivity apps for email, calendar, contacts, and content that also protects critical work data with data loss prevention policies in place.

Workspace ONE establishes trust between the user, device, and enterprise for one-touch authentication into work apps for a secure and seamless experience. End users can navigate to their centralized app catalog and gain instant access to their work data. SSO can also be applied to the installed managed applications in the work profile on the device. Workspace ONE can enforce authentication strength and restrict access to non-compliant devices.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: FY20-5749-VMW-WKSPONE-ANDROID-DS-USLET-20200128 1/20